The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 17, No. 1, pp.13-18, Feb. 28, 2017. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2017.17.1.13
JIIBC 2017-1-2

비디오 암호화를 위한 여원 최대길이 셀룰라 오토마타

Complemented Maximum-Length Cellular Automata Applied on Video Encryption

이고용*, 조성진**, 김석태***

Gao-Yong Li*, Sung-Jin Cho, Seok-Tae Kim*****

요 약 인터넷기술의 발전에 따라 데이터를 보호하려는 연구가 점점 중요하게 되었다. 데이터를 보호하는 방법의 하나로서 본 논문에서는 여원 MLCA(Complemented Maximum Length Cellular Automata) 기법을 이용한 비디오 암호화 방법을 제안한다. 먼저 CA규칙 90/150을 이용해 여원 MLCA의 상태 전이행렬 T를 만든 후, 2D 여원MLCA의 기저영상을 생성한다. 다음, 비디오영상을 다중프레임으로 나눈다. 마지막으로 여원 MLCA 규칙을 이용하여 생성한 기저영상과의 XOR 연산으로 최종 암호화된 비디오영상을 얻게 된다. 이러한 방법은 영상 데이터를 시각화하기 위한 영상의 기본 정보인 픽셀의 값을 변환시키기 때문에 기존의 암호화 방법보다 향상된 암호화 결과를 얻을 수 있다.

Abstract With the advancement of internet technology, the importance of data protection is gaining more attention. As a possible data protection solution, we propose a novel video encryption method using complemented maximum-length cellular automata (C-MLCA). The first step for encryption is to use 90/150 CA rule to generate a transition matrix T of a C-MLCA state followed by a 2D C-MLCA basis image. Then, we divide the video into multiple frames. Once, we perform exclusive-OR operation with the split frames and the 2D basis image, the final encrypted video can be obtained. By altering values of pixel, the fundamental information in visualizing image data, the proposed method provides improved security. Moreover, we carry out some computational experiments to further evaluate our method where the results confirm its feasibility.

Key Words : video encryption, complemented maximum-length Cellular Automata, 90/150 CA rule.

Ⅰ. INTRODUCTION

With the rapid development of Internet, the usage of video files has become more frequent. It is important to protect the privacy of the authorized users in communication and to guarantee the legal data access in storage of data[1-3]. Our novel video encryption approach is one possible way to ensure the video files' security.

For video encryption, there have been a lot of research and methods. Encryption scheme based on secret Keys is intensively used in modern security

*정회원, 부경대학교 정보통신공학과
**정회원, 부경대학교 응용수학과
***정회원, 부경대학교 정보통신공학과

접수일자 : 2016년 11월 28일, 수정완료 : 2016년 12월 28일
게재확정일자 : 2017년 2월 3일

Received: 28 November, 2016 / Revised: 28 December, 2016 / Accepted: 3 February, 2017

***Corresponding Author: setakim@pknu.ac.kr
Dept. of information and communications Eng., Pukyong National University, Korea

systems to ensure data integrity. Pareek proposed an encryption scheme using the chaotic logistic map [4] and Tong used XOR operation and new chaotic function to generate a random number sequence[5]. To improve encryption security, some researchers try to use complex key structures such as double random phase keys and chaotic sequence keys; however, the encryption is usually not robust [6-9]. Moreover, it is likely to impose a heavy burden on the practical encryption system when a large amount of hologram data processing is required. Of course, there exist other encryption methods used. GC Langelaar proposed the DCT method applied to encoding[10]. Nonetheless, encryption and decryption processes are still slow and complicated.

Some researchers proposed Zig-Zag permutation [11] applied to video encryption; however, this algorithm cannot withstand the known-plaintext attack. Zeng and Lei [12] also proposed the selective encryption DWT which only encrypt a subset of the data. The method can reduce the amount of data to encrypt while preserving a sufficient level of security.

Cellular automata (CA) have been of theoretical interest since the pioneering work of Von Neumann in 1940s. CA are dynamical systems in which space and time are discrete. Pseudorandom number generation by CA has been an active field, including Monte Carlo techniques, Brownian dynamics, and stochastic optimization methods. With the advent of massively parallel scientific computation, the parallel generation of pseudorandom numbers appeared, as measured by appropriate statistical tests. Moreover, when very long sequences of random numbers are needed, CA provides a good solution to this problem as it allows to rapidly produce high-quality random-number streams.

We propose a novel video encryption method using complemented maximum-length cellular automata (C-MLCA). In this scheme, we first generate 2D C-MLCA basis image by 90/150 CA rules. Then we divide the video into multiple frames. The following step is to select all frames and to do the XOR operations with 2D basis image. In the decryption process, all the encrypted images do same XOR operation with 2D basis image. Then we obtain the decrypted frames. Owing to the large dimension of the CA key space, the proposed scheme can provide high security.

Ⅱ. ENCRYPTION APPROACH BASED ON COMPLEMENTED MAXIMUM-LENGTH CELLULAR AUTOMATA

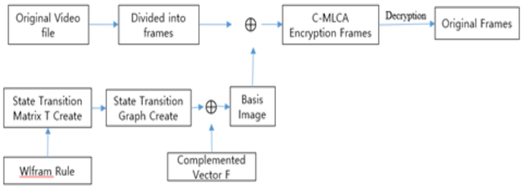


그림 1. 암호화 방법의 흐름도
Fig. 1. The flow chart of encryption algorithm

The encryption process of proposed scheme is shown in Fig.1. which consists of five steps of operations:

Step 1. By using transition matrix T of 90/150 CA rule, the C-MLCA encryption image is generated. This basic image is our encryption key.

Step 2. The video file to be encrypted is decomposed into individual frames. In this way, we can make the corresponding operation for each frame.

Step 3. Do the XOR operation with the basic image and frames. The obtained image after the operation is the result of finalized encryption.

Step 4. The operation here is decryption. Do an XOR operation on the encrypted image.

Step 5. Recombine all the decryption frames. We can get the original file.

CA are dynamical systems [13] in which space and time are discrete. And the CA evolution is expressible in the form:

$$a_{i(t+1)} = F[a_{i-1(t)}, a_{i(t)}, a_{t+1(t)}] \tag{1}$$

If f(x) represents the state of the CA at the t^{th} instant of time, the next state is by transition equation:

$$f_{t+1}(x) = T \times f_c(x) \tag{2}$$

The global state appearing after the m^{th} iteration is

$$f_{t+m}(x) = T^m \times f_t(x) \tag{3}$$

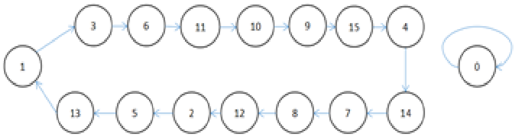
To derive its next state, a CA employs on XOR logic.

T is called the state-transition matrix, a state s0 is called a cycle state if there exists an inter p such that

$$S_0 = T^p \times S_0 \tag{4}$$

The smallest integer p that satisfies Eq.4 is called cycle length of the CA. If length of an n-cell CA is $2^n - 1$,it will be called Maximum Length Cellular Automata [14]. Here is the example of the concept that we introduced:

$$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$



Characteristic polynomial of T is $x^4 + x^3 + 1$ and the lowest value k for this polynomial dividing $x^k + 1$ is $2^4 - 1$.

The complemented CA evolution is expressible in the form:

$$\overline{x_{l(t+1)}} = f[x_{i-1(t)}, x_{i(t)}, x_{i+1(t)}] \oplus F(x) \tag{5}$$

We consider a three-site neighborhood, dual-state, one dimension CA. f is a Boolean function where it defines the rule, F is complemented vector and ⊕ devotes exclusive-OR logic.

Here the CA rules about i^{th} cell state at time t+1 where ⊕ denotes XOR operation:

Rule 90:

$$q_{i(t+1)} = q_{i-1}(t) \oplus q_{i+1}(t) \tag{6}$$

Rule 150:

$$q_i(t+1) = q_{i-1}(t) \oplus q_i(t) \oplus q_{i+1}(t) \tag{7}$$

And here is the detail about rule 90/150:

Neighborhood state:

	111	110	101	100	011	010	001	000	
next state:	0	1	0	1	1	0	1	0	(Rule 90)
next state:	1	0	0	1	0	1	1	0	(Rule 150)

Ⅲ. SIMULATION RESULTS AND DISSCUSION

In this encryption scheme, a raw video file is used (30 frames/s). We divided the video into separate frames. We use the famous image Lena as an example and the frames are presented in Fig.2.

(a) (b) (c)

그림 2. 첫 번째 프레임 (a), 두 번째 프레임 (b), 세 번째 프레임 (c)
Fig. 2. The first frame (a), second frame (b) and third frame(c)

In our scheme, we encrypted the frames based on C-MLCA. First of all, we need the key of encryption and generated basis images. The linear MLCA and C-MLCA basis images are as following:

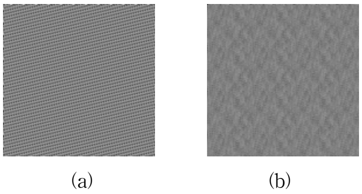


그림 3. 2D 기저 영상
Fig. 3. 2D basis images

Fig.3 (a) and (b) show the MLCA basis image and the C-MLCA basis image with 256×256pixels, respectively. By using the MLCA basis image, we can obtain the encrypted images as following:

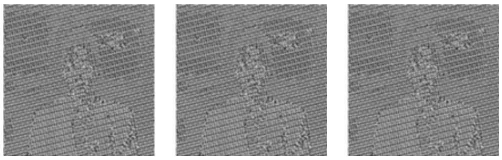


그림 4. MLCA를 이용한 암호화 영상
Fig. 4. Encrypted images by using MLCA.

However, from the results of Fig.4, we can see that the profile of image can still be recognized from the encrypted image. While every pixel in Fig.4 has been encrypted, the pixel that was the same in the original image are the same in the MLCA-encrypted version. Obviously, this is not very safe for practical applications. So we provide a better way to encrypt it for protecting the data.

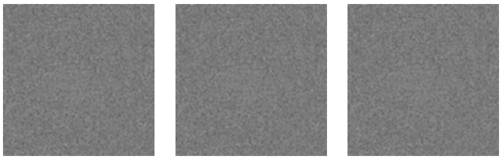


그림 5. C-MLCA를 이용한 암호화 영상
Fig. 5. Encryption images by using C-MLCA.

To address the problem, we introduce the C-MLCA. Fig.5 shows the encrypted image based on the proposed method, the qualities of the encrypted images have obviously improved. By doing so, we can achieve the purpose of encryption.

The benefit of C-MLCA Mode is that identical plaintext will not yield identical ciphertext. This is dramatically illustrated by comparing sample images encrypted using MLCA mode which appear in Fig.4 with the images encrypted in C-MLCA mode which appear in Fig. 5. Then, we can achieve the purpose of encryption. When you lock a door, you must know how to open it. Fig.6 shows the decrypted images of the proposed scheme. As the decryption is implemented using XOR operation, the pixels of original and decrypted frames are the same.

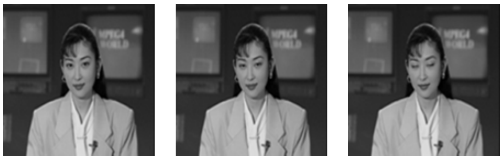


그림 6. 복호화된 영상
Fig. 6. Decrypted images

Ⅳ. ESTIMATE PARAMETERS

To evaluate the decryption quality of the proposed scheme, we introduce two parameters to provide completed of information of the pixels distribution respect to the original image. The bit correct ratio (BCR) and peak signal to noise ratio (PSNR) are introduced. The BCR and PSNR in a high value correspond to a great similarly between the decrypted image and the original image. Meanwhile, the BCR and PSNR in a low value indicate the dissimilarly between the decrypted image and the original image.

$$PSNR = 10log_{10}\left(\frac{255^2}{MSE}\right) \tag{8}$$

$$MSE = \left(\frac{1}{w \times H}\right)\sum_{i=1}^{W}\sum_{j=1}^{H}\left(x_{ij} - x'_{ij}\right)^2 \qquad (9)$$

$$BCR = \left(1 - \frac{\sum_{i=1}^{L_M}(w_i \oplus w'_i)}{L_M}\right) \times 100\% \qquad (10)$$

표 1. 평가 파라미터
Table 1. Estimate Parameters

Parameter	MLCA	C-MLCA
PSNR(dB)	12.356	11.357
BCR(%)	0.1593	0.0143

As can be seen from the data in the table 1, the experimental results are satisfactory. The typical BCR value of the proposed C-MLCA scheme obtained as 0.0143% and PSNR value is recorded as 11.357dB. The BCR and PSNR values of the conventional MLCA-based method are recorded as 0.1593% and 12.356dB, respectively. Analysis the results, the BCR and PSNR of the proposed scheme has improved compared with the conventional MLCA-based method.

A C-MLCA encryption system provides a high degree of security because of the 2D key space, CA gateway values, the rule, cell numbers, boundary conditions, etc.

표 2. 암호화 시간
Table 2. Encryption time values

Video length	Encryption time	Time required per frame
15s	20s	0.0444s

Table 2 shows the time values for the encryption. It takes a short amount of time to implement the process. Moreover, the key space is very wide. So we can achieve a relatively high security.

Ⅴ. CONCLUSION

In this paper, a novel video encryption method using C-MLCA is proposed. The first step for encryption is to use 90/150 CA rule to generate a transition matrix T of a C-MLCA state followed by a 2D C-MLCA basis image. Then, we divide the video into multiple frames. Once, we perform exclusive-OR operation with the split frames and the 2D basis image, the final encrypted video can be obtained. By altering values of pixel, the fundamental information in visualizing image data, the proposed method provides improved security. Moreover, we carry out some computational experiments to further evaluate our method where the results confirm its feasibility.

The feasibility of the method has been verified as the images provide high quality and are free of data loss. The experiments show that this encryption method provides greatly improved encryption speed and security.

References

[1] Won Ho, et al., “Performance analysis of the encryption algorithms in a satellite communication network based on H-ARQ,” IIBC, The Journal of The Institute of Internet, Broadcasting and Communication Vol.15, No.1, pp.45-52, 2015
DOI: https://doi.org/10.7236/JIIBC.2015.15.1.45

[2] Y. S. Im and E. Y. Kang, “MPEG-2 video watermarking in quantized DCT domain,” The Journal of The Institute of Internet, Broadcasting and Communication(JIIBC), Vol.11, No.1, pp. 81-86, 2011

[3] Jeon, S. Kang and H. Yang, “Development of security quality evaluate basis and measurement of intrusion prevention system,” Journal of the Korea Academia-Industrial cooperation Society (JKAIS), Vol.11, No.1, pp. 81-86, 2010
DOI: https://doi.org/10.5762/KAIS.2010.11.4.1449

[4] N. K. Pareek, Vinod Patidar and K. K Sud, “Image encryption using chaotic logistic map,” IVC. Vol.24, No.9, pp. 926-934, 2006
DOI: https://doi.org/10.1016/j.imavis.2006.02.021

[5] X. Tong and M. Cui, "Image encryption with compound chaotic sequence cipher shifting dynamically," IVC.26, pp. 843-850, 2007
DOI: https://doi.org/10.1016/j.imavis.2007.09.005

[6] X. Li, S. J. Cho and S. T. Kim. "A 3D image encryption technique using computer-generated integral imaging and cellular automata transform," Optik, Vol.125, pp. 2983-2990, 2014
DOI: https://doi.org/10.1016/j.ijleo.2013.12.036

[7] Li XW and Kim ST. "Optical 3D watermark based digital image watermarking for telemedicine," Opt Laser Eng, Vol. 51, pp.1310-1320, 2013
DOI: https://doi.org/10.1016/j.optlaseng.2013.06.001

[8] J. Sang, et al. "Security analysis and improvement on a double-random phase-encoding technique based information hiding method," Opt Commun.,Vol.282, pp.2307-2317, 2009
DOI: https://doi.org/10.1016/j.optcom.2009.02.068

[9] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt Lett., Vol. 20, pp.767 - 769, 1995
DOI: https://doi.org/10.1364/OL.20.000767

[10] GC Langelaar and RL Lagendijk. "Optimal differential energy watermarking of DCT encoded images and video," Vol.10, No.1, pp. 148-158, 2001
DOI: https://doi.org/10.1109/83.892451

[11] L. Tang, "For encryption and decrypting MPEG video data efficiently," in Proceeding of the Forth ACM International Conference on Multimedia; pp. 55-61, 1998
DOI: https://doi.org/10.1145/244130.244209

[12] W. Zeng and S. Lei, "Efficient frequency domain selective scrambling of digital video," IEEE Transactions on Multimedia, Vol.5, No.1, pp. 118-129, 2003
DOI: https://doi.org/10.1109/TMM.2003.808817

[13] Xiao-Wei Li and Seok-Tae Kim, "Optical 3D water mark based digital image watermarking for telemedicine, Optics & Lasers in Engineering," Vol.51, pp. 1310-1320, 2013
DOI: https://doi.org/10.1016/j.optlaseng.2013.06.001

[14] X. W Li, J. S Yun, S .J. Cho and S. T. Kim, "Watermarking based on complemented MLCA and 2D CAT," KIMICS, Vol.9, No.2, 2011
DOI: https://doi.org/10.6109/jicce.2011.9.2.212

저자 소개

이 고 용(정회원)

• 2014년 : Dalian Ocean University of China,(공학사)
• 2016년 : 부경대학교, 정보통신공학과 졸업(공학석사)
<주관심분야 : 영상처리, 영상 암호화, Cellular automata>

조 성 진(정회원)

• 1979년 : 강원대학교 수학교육과 졸업 (이학사)
• 1981년 : 고려대학교 대학원 수학과 졸업(이학석사)
• 1988년 : 고려대학교 대학원 수학과 졸업(이학박사)
• 1988년 ~ 현재 : 부경대학교 응용수학과 교수
<주관심분야 : 셀룰라 오토마타론, 정보보호>

김 석 태(정회원)

• 1983년 : 광운대학교 전자공학과졸업 (공학사)
• 1988년 : Kyoto Institute of Technology, 전자공학과졸업(공학석사)
• 1991년 오사카대학교 통신공학과졸업(공학박사)
• 1999년 Univ. of washington, USA, 방문교수
• 2006년 : Simon Fraser Univ., Canada, 방문교수
• 1991년 ~ 현재 : 부경대학교 정보통신공학과 교수
<주관심분야 : 영상처리, 영상 암호화, Cellular automata>

This work was supported by a Research Grant of Pukyong National University (2015 year).